UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,306	09/27/2006	Paolo Milani Comparetti	09952.0074	3388

22852 7590 03/22/2011

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
03/22/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/594,306	MILANI COMPARETTI ET AL.	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *39,41-57 and 59-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *39,41-49,55-57,59-68 and 74-77* is/are rejected.

7)☒ Claim(s) *50-54 and 69-73* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 1/28/2011 was received and considered.

2. Claims 39, 41-57 and 59-77 are pending.

Response to Arguments

3. Applicant's response has successfully overcome the previous §101 rejections and objection to the specification.

4. Applicant's response necessitates further consideration. In light of Applicant's amendments, claims 50-54 and 69-73 are objected to as being allowable dependent claims and would be allowed if combined with the elements of the based claim and all intervening claims.

5. Applicant's arguments with respect to claims 39, 41-49, 55-57, 59-68 and 74-77 have been considered but are moot in view of the new ground(s) of rejection.

6. The Examiner believes the prior art provides a showing of associating data flows with application layer protocols, independent of ports. Roesch teaches that using data in packets, applications running on the computer can be established; being that the applications reflected in the traffic, the Examiner maintains that this is sufficient to show determining a protocol used by an application. It is noted that determination of a particular protocol was not claimed, only that a protocol involved in monitored data flows was determined. In that all traffic is associated with a protocol and is sent by applications on the target, as evidenced by a determination of the application from the traffic, it is believed Roesch provides a sufficient prior art showing. However, based on the amendments and their application especially to the rejections of the independent claims, Graham is provided, with the exception of the above allowable claims. Graham discloses this in the context signatures (Figs. 4-5 and Figs. 10-11). Further, the Examiner notes that the Hernacki reference teaches a system that performs "the identification of application protocol" (col. 3, lines 2-3) using heuristics to determine the application associated with a

flow that "could identify protocols without relying on the port mapping conventions" (col. 1, lines 63-64). Therefore, the Examiner believes the independent claims, as recited are not yet allowable over the prior art of record.

Claim Objections

7. Claims 41-43, 46, 51 and 55-56 are objected to because of the following informalities:

a. Regarding claims 41-43, 46, 51 and 55, the limitation "said step of detecting information on application layer protocols" should be replaced with "said step of detecting information relating to application layer protocols".

b. Regarding claim 56, the limitation "based on said information on application layer protocols" should be replaced with "based on said information relating to application layer protocols".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 39, 41-49, 56-57, 59-68 and 75-77 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 7,237,264 to Graham et al. (**Graham**).

Regarding claims 39, 57 and 76-77, Graham discloses monitoring data flows in said network (monitoring network traffic, col. 4, lines 44-50); detecting information relating to application layer

protocols associated with said monitored data flows independently of said network ports (detecting commands, col. 5, lines 32-34, Fig. 10); and providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols (knowing that the protocol is FTP, without using ports, and knowing that certain commands can process filenames, "RETR /etc/passwd" will trigger, but not the "SYST" command, col. 5, lines 24-42) independently of any predefined association between said network ports and said application layer protocols (uses command data within the packet payload to determine application protocol, Fig. 10).

Regarding claims 41 and 59, Graham discloses wherein said step of detecting information on application layer protocols comprises passive observation of network traffic (monitoring network traffic, col. 4, lines 44-50).

Regarding claims 42 and 61, Graham discloses wherein said step of detecting information on application layer protocols comprises using signature-matching techniques (Figs. 10-11).

Regarding claims 43 and 62, Graham discloses wherein said step of detecting information on application layer protocols in said data flows comprises the step of identifying at least one protocol in a given data flow (Fig. 11, col. 8, lines 1-5).

Regarding claims 44 and 63, Graham discloses wherein said step of providing intrusion detection comprises signature-based detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on said information on application layer protocols (Fig. 11, determining FTP from commands, col. 5, lines 24-42, col. 10, lines 7-18).

Regarding claims 45 and 64, Graham discloses providing intrusion detection based on a plurality of predefined sets of analysis tasks and misuse signatures (Fig. 10) for a plurality of said protocols (detecting context includes detecting the protocol, col. 5, line 55 – col. 6, line 30; see also Fig. 5 shows payloads defining different protocols, Figs. 10-11, col. 1, lines 10-57), and comprises selecting out of said plurality a set related to at least one protocol in a given data flow (determining FTP, col. 5, lines 1-8) and

at least one of the steps of: performing over said data flow the selected set of analysis tasks (monitoring state, col. 5, lines 32-42); and performing signature matching over said data flow against the selected set of misuse signatures (Fig. 10).

Regarding claims 46 and 65, Graham discloses wherein said steps of detecting information on application layer protocols and providing intrusion detection are performed within the same functional module and employing the same functional blocks of packet capture, preprocessing and signature matching (single node, col. 4, lines 44-50, col. 6, lines 23-30).

Regarding claims 47 and 66, Graham discloses wherein said signature-matching is performed by comparing monitored traffic with a set of protocol detection signatures (detecting context includes detecting the protocol, col. 5, line 55 – col. 6, line 30; Fig. 5 shows different payloads for detecting protocols) having the following characteristics: the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system (Fig. 5), and each said signature specifies a respective protocol that is detected if the signature is triggered (Fig. 5).

Regarding claims 48 and 67, Graham discloses wherein each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol (Fig. 5).

Regarding claims 49 and 68, Graham discloses using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior (Fig. 11).

Regarding claims 56 and 75, Graham discloses wherein said step of providing intrusion detection based on said information on application layer protocols comprises the steps of: establishing a network policy (signatures, Fig. 11), and generating a security event whenever a protocol is detected in violation of said network policy (generate an alert when signature matches, Fig. 11).

Regarding claim 60, Graham discloses wherein said module is a sniffer (packet interception and monitoring, col. 4, lines 44-50).

10. Claims 55 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Graham**, as applied to claims39 and 57 above, in view of U.S. Patent 6,182,146 to Graham-Cumming, Jr. (**Graham-Cumming**).

Regarding claims 55 and 74, Graham lacks wherein said step of detecting information on application layer protocols in said data flows comprises producing a map of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection is performed on said associated network ports. However, Graham-Cumming teaches that some application protocols allow deviation from standard ports and teaches classifying flows based on data in the payload (col. 6, lines 13-55) and maintaining a map of associations between application layer protocols and network ports present in the network (col. 5, lines 53-57). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Graham to include producing a map of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection is performed on said associated network ports. One of ordinary skill in the art would have been motivated to perform such a modification to maintain a record of which protocols are being used on which ports, as taught by Graham-Cumming.

Allowable Subject Matter

11. Claims 50-54 and 69-73 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

c. Regarding claims 50 and 69, the prior art of record fails to teach or disclose, either alone or in combination, leaving out (excluding) signatures exclusively matching a pattern in client behavior, in combination with the remaining elements of the claims.

d. Regarding claims 51 and 70, and 52-54, 71-73 by dependence, the art of record teaches determining a server running (Roesch, col. 14, lines 42-44; Graham teaches determining FTP, Fig. 5). However, the prior art of record fails to teach or disclose, either alone or in combination, characterizing and classifying data flows related to each server application in said network, in combination with the other elements of the claims.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 17, 2011
/Michael J Simitoski/
Primary Examiner, Art Unit 2439